Übersetzung

- Information Leaflet on Data Protection -

Dear Sir or Madam,

The events within the scope of the G8 summit in 2007 as well as of the EU Presidency of the Federal Republic of Germany during the first six months of 2007 are occasions of international importance.

A peaceful and trouble-free course of the events is in the interest of all parties involved. By law, the Bundeskriminalamt has been assigned the task of protecting international guests of the Federal Government. To guarantee their safety, access to the respective venues is only granted to persons who were accredited.

The accreditation requires a reliability check. This reliability check is a security measure taken by the organiser. In all cases, the organiser is the Federal Government.

As the accreditation procedure is necessarily connected with a processing of your personal data, which cannot be done unless you give your explicit approval, we would like to explain in greater detail what will happen to your personal data:

The data obtained in the course of the accreditation procedure are electronically recorded and stored on a server at the Bundeskriminalamt or, if necessary, on servers at the other authorities respectively involved. All personal data stored in the accreditation system will be deleted by early July 2008 at the latest. This storage period is expected to guarantee a professional handling of inquiries made by applicants about their own personal data stored and of queries and/or complaints about accreditation granted or not granted.

The data provided by you is exclusively used by the Bundeskriminalamt for the decision on granting the right of access and for monitoring the observation of corresponding restraints. The obtaining, processing and using of personal data therefore serves to guarantee the security of the respective event.

If you wish to assert your data protection rights (in particular information and correction rights), you can contact the entity responsible under data protection law. This entity is the organiser.

You can freely decide whether to give your consent to the processing of data as depicted in this text and in particular to the reliability check. But if you refuse to do so, accreditation cannot be granted. The data especially marked as optional, however, can be dispensed with, because it is not absolutely essential to dealing with the application for accreditation; nevertheless, this information would be helpful to us.

You also have the right to later withdraw your approval previously given. In this case, accreditation granted to you till then would have to be revoked. Your data will then remain stored in the accreditation database until the aforementioned period elapsed but it will be blocked from further processing. This storage period serves to professionally handling inquiries made by applicants about their own personal data stored and to guarantee queries and/or complaints about accreditation not granted. If the reliability check has already been accomplished by the security authorities (see the following chapter in this respect) at the time when the approval is withdrawn, this will not exert any influence on the continued storage of your data there until the period mentioned in the information leaflet on data protection elapsed.

Reliability check

In connection with the accreditation, checks are to be made to ascertain whether the authorities involved (police, Offices for the Protection of the Constitution, Federal intelligence Service) hold information that pose an obstacle to granting access to the respective event. (reliability check). To this end, an abstract of the data collected (surname, first name, name at birth or another name, date of birth, place of birth, sex, nationality as given in the identity document, postal code, place of residence, street, house no., federal state, country, type and number of the identity document, name of the event, purpose of the event, registration number) is to be made available in electronic form to the Landeskriminalamt (State Criminal Police Office) of the Federal State where you currently have your residence, as well as to the Bundeskriminalamt, the Federal Police (the former Federal Border Guard), the Federal Office for the Protection of the Constitution and the Federal Intelligence Service (if foreign nationals residing abroad apply for accreditation) with a view to carrying out a reliability check. On the basis of the data, the aforementioned authorities make checks to determine whether there is information stored in their databases posing an obstacle to your presence in the security area for security reasons. The Federal Office for the Protection of the Constitution ensures that queries are made of the data network operated by the offices for the protection of the constitution at federal and state level. The Federal Intelligence Service checks the data with links to foreign countries.

The State Criminal Police Office that is responsible for you and the Federal Police as well as the Federal Office for the Protection of the Constitution and the Federal Intelligence Service separately inform the Bundeskriminalamt of the results of their checks. The Bundeskriminalamt compiles their results and the results of its own checks and submits a comprehensive conclusive recommendation to the respective organiser.

<u>Data used for making checks:</u>

Your data is checked against various databases operated by police services for the purpose of criminal prosecution and warding off danger. These are databases part of which are only separately operated by the police services at federal and state level but also databases that are jointly used (data networks).

In particular, these are databases containing information on criminal offenders/offences where penal convictions but also investigative proceedings still pending as well as discontinued and penal proceedings without conviction by a court are stored or these are state security databases (containing information relating to offences with a political background or about the membership of organisations or associations banned in Germany, such as the Kurdish Workers' Party (PKK) or the German right-wing extremist Nationalist Front (*Nationalistische Front*; NF)).
The storage period of data in these databases is defined by the provisions of the police laws at federal and state level. The period depends on the respective individual case in consideration of the seriousness of the charge and the court decision, if available, as well as on the fact whether the person concerned was an adolescent (under 18 years old) or an adult (18 years of age and over) at the time of the offence. As a rule, the storage period in case of felonies and specific serious misdemeanours as well as in case of other criminal offences of supraregional significance is ten years, if committed by adults, and five years, if committed by adolescents. In case of less serious crime, the storage period for data of adults is five years. If the perpetrators are adolescents, the storage period is appropriately shorter. In cases of minor significance, the review periods are reduced to three years. If a new relevant offence is additionally stored with regard to a person prior to the expiry of the review period, the storage

period may be prolonged with the information as yet stored being retained.

We would like to point out that the information stored in police databases can be more extensive than the information held in the Federal Registry of Judicial Antecedents, because, in principle, procedures discontinued by courts/public prosecutor's offices or completed without a conviction may also be stored.

When checked by the **agencies responsible for the protection of the constitution** your data is searched against the information system of the intelligence services (NADIS), a joint database containing references to records where information can be retrieved, which is operated by the agencies responsible for the protection of the constitution.

The reasons for the storage and the storage period of data in NADIS are defined by the provisions of the constitutional protection laws at federal and state level. As a rule, the storage period in case of minors is five years and in case of adults, it is ten or fifteen years after relevant information had last been stored.

The **Federal Intelligence Service** checks your data, if you are the holder of a foreign nationality and you have your residence abroad. In those cases, the Federal Intelligence Service will search your data against information available on international terrorism and organised crime. Pursuant to section 5, subsection 1 of the Law on the Federal Intelligence Service in connection with section 12, subsection 3 of the Law on the Protection of the Constitution it shall be considered in the course of the continued processing of orders, but after five years at the latest, whether to update or delete stored personal data. Only if it is ascertained as a result of this consideration that the storage of this data is no longer required, will the data be deleted.

Criteria that are essential to the decision:

The objective of the reliability check carried out by police authorities is to guarantee a secure and trouble-free course of the event. Persons who are the subject of fears that they pose a risk to the overall event are to be prevented from any activities in security-related areas. As a matter of principle, the accreditation is therefore rejected without providing reasons for the assessment, if the checked person was convicted of an offence of considerable significance with final and binding effect and the conviction was three years before at the latest. These include, in particular:

- felonies (criminal acts, which are subject to a minimum sentence of one year or above) targeting the life and health of persons

- misdemeanours (criminal acts, which are subject to a minimum sentence of less than one year or a fine), which, in individual cases, are capable of braking the peace under law according to their type and seriousness , if

    a) they target life, health or freedom of one or more persons or
    b) were committed in the field of illicit trafficking in arms and narcotic drugs or
    c) in the field of state security.

If you were repeatedly sentenced for other offences of considerable significance with final and binding effect, police authorities will give a negative recommendation, if this appears to be appropriate upon a careful consideration of all circumstances.
In individual cases, it can also be appropriate to give a negative recommendation if a person was repeatedly convicted for minor offences.

In order to perform a threat assessment, it is required in all cases to take into account all police information available on the applicant.
Other information, e.g. on pending or discontinued investigative proceedings or penal proceedings without a conviction by a court, can lead to a negative recommendation, if this appears to be appropriate upon careful consideration of the respective case. The same applies if information involving state security, narcotic drugs or organised crime are available on a person and give rise to the assumption that he/she will commit such offences in the future.

In principle, the agencies responsible for the protection of the constitution will recommend a rejection of the accreditation, if information is available resulting in factual indications that

a) the applicant will commit violent offences,
b) the applicant previously committed one or more acts of violence, which are capable of breaking the peace under law according to their type and seriousness,
c) the applicant is part of violence-prone efforts or firmly supports such efforts,
d) the applicant will call for acts of violence or called for such acts in the past.

The same applies if factual information is available on the applicant indicating that he/she will commit acts with extremist background, which are capable of negatively affecting the freedom of will and action of a person under protection.

The aforementioned criteria merely serve as an orientation for the recommendations to be given by the agencies responsible for the protection of the constitution; what is decisive is the individual case. Not every entry in NADIS automatically leads to a rejection.

In principle, the Federal Intelligence Service will recommend a rejection of the accreditation, if information is available in the data records on international terrorism or organised crime resulting in factual indications that

a) the applicant will commit violent offences,
b) in the past, the applicant committed one or more terrorist acts of violence abroad, which are capable of breaking the peace under law according to their type and seriousness,
c) the applicant is part of violence-prone efforts abroad or firmly supports such efforts,
d) the applicant will call for acts of violence or called for such acts abroad in the past.

The same applies if factual information is available on the applicant suggesting there is a risk of him/her committing terrorist or other acts with extremist background, which are capable of jeopardising/negatively affecting the public security or Germany's reputation in the world.

The aforementioned criteria merely serve as an orientation. What is decisive is the individual case. Not every entry in the data records on international terrorism or organised crime automatically leads to a rejection.

Procedure

Please note that the police authorities exclusively inform the respective organiser of the results of their reliability check. Neither you nor your employer (if you are employed by a service company and your employer applied for the accreditation on your behalf) are directly informed of the results. The assessment performed by the security authorities serves the organiser as a basis for their decision on granting accreditation or taking an adverse decision:

- If part of the information provided is incorrect, e.g. if an incorrect date of birth was given, the Bundeskriminalamt will advise the respective organiser and/or applicant accordingly. The organiser/applicant will then ask you (or your employer, if they filled in your application) to correct the incorrect data.

- If there are "no reservations" about granting an accreditation after the data had been checked by the authorities involved, the organiser will be informed accordingly.

- If there are "reservations" about granting an accreditation after the data had been checked by the authorities involved, the organiser will be informed accordingly (without stating reasons). Such reservations lead to the rejection of the application for accreditation.

If the organiser rejects your accreditation because of reservations expressed by the authorities involved about your reliability, you (but not your employer) have the possibility to contact the State Criminal Police Office in the federal state where you have your residence and/or the Bundeskriminalamt if you reside abroad, in order to enquire about the reasons. You can put forward your objections there as well. If possible, your complaint will then be forwarded to the security authority/authorities giving the negative recommendation. Your objections are considered and the recommendation given to the organiser is modified, if possible. If your complaint was not allowed, you will be notified accordingly. You can assert your other data protection rights (in particular, information and correction rights) in a corresponding manner - - if it is about data processing at the security authorities. In connection with the exercise of your data protection rights you can contact the appropriate state data protection authority and/or the Federal Commissioner for Data Protection and Freedom of Information.

The data collected in connection with the reliability check will be stored at the authorities mentioned above for a period of three months starting with the official end of the EU Presidency, in case the application for accreditation was not rejected, otherwise the data will be stored for a period of one year, in order to be in a position to later determine - if needed - what aspects were essential to the decision. Upon expiry of the aforementioned periods, the data will be deleted. The data are blocked from general access till its expiry.

Declaration of Consent

Name in printed characters

_____

Organiser of the event

_____

Employer

_____

Event

_____

On the basis of the information leaflet on data protection, I herewith consent to the data processing, in particular the reliability check to be made by police authorities and agencies responsible for the protection of the constitution at federal and state level and by the Federal Intelligence Service in the case of foreign nationals residing abroad as well as to information being exchanged to this end between the police and the organiser of an event.

Place Date Signature

_____